REMARKS

Reconsideration of the present application, as amended, is respectfully requested. Claims 1, 2, 14, and 17 have been amended. No claims have been cancelled or added.

Examiner rejected claims 1, 5, 6, 8, 9, 11-14, 17, 23, 24, 26, 27, and 29-31 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,853,988 to Dickinson et al. Examiner rejected claims 2-4 and 20-22 under 35 U.S.C. §103(a) as being unpatentable over Dickinson as applied to claim 1 above, and further in view of U.S. Patent No. 6,233,685 to Smith et al.

The Examiner notes that Dickinson does not teach or suggest generating a random record ID for the user. The Examiner suggests that the combination with Smith remedies this shortcoming of Dickinson. Applicants respectfully disagree.

First, Dickinson and Smith cannot be logically combined. Dickinson is concerned about providing third party authentication. In contrast, Smith's focus is on establishing the integrity/untampered state of a secure device. It uses activated tamper responses, with key regeneration. One of skill in the art in third party authentication would not look to secure devices. Furthermore, the Examiner simply states that it would have been obvious to have modified Dickinson to have randomly generated public/private key pairs, without showing any such suggestion within the reference itself.

Therefore, Applicants respectfully submit that Dickinson and Smith cannot be combined. Furthermore, even in combination, Dickinson and Smith do not make the claims, as amended, obvious.

The Examiner suggests that Smith teaches, at column 8, line 66 to column 9, line 19, the concept of generating a random record ID for a user. The referenced section of Smith states:

> The device then uses an internal source of true randomness to generate its initial keypair. The keypair includes a random public key and a random private key (104). It is advantageous that the internal source be a true random number generator. The device stores the private key internally, in secure memory. The secure memory is protected by the tamper-response circuitry (106). The device exports its public key (108) to the certifying authority. At this point, the certifying authority verifies that the public key really originates from an authentic, untampered device (110). It is advantageous that the manufacturer be the certifying authority so that this verification follows directly from the fact that this device was just built and is still inside the manufacturer's vault. However, the certifying to be authenticated. In one implementation the certifying authority does this by sending the certificate to the device (118). The device may thenceforth be requested to present the certificate and/or the information contained in it to the requesting party. In an alternate implementation, the certifying authority publishes the certificate in a public repository.

Clearly, this section of Smith does not teach or suggest a random record ID. Furthermore, Smith is authenticating a device. Therefore, in Smith there is absolutely no motivation or logic to disassociating the name from the authentication data. For humans, separating authentication data from user name ensures that a hacker cannot obtain enough information to cause harm. Since the association of record ID with user name is not stored with the system, a hacker would have to compromise both the user's system and the server in order to obtain information sufficient to cause harm.

Claim 1, as amended, recites

> A method of authenticating a client, the method comprising in an authentication server:
> receiving a record ID for a user, the record ID being a random record ID generated for tracking authentication data, and a one-time key generated by a third party server and encrypted with a user's public key by the server;
> receiving the user's authentication data from the client;

determining if the user's authentication data matches the record ID; and

if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client.

(Claim 1, as amended). Neither Dickinson nor Smith teaches or suggests a random record ID generated for tracking authentication data. The Examiner notes that Dickinson does not teach or suggest this limitation. There would be no logical use for such a separation in Smith, since the device ID is sufficient for such identification. Therefore, claim 1, and claims 2-13 which depend on it, are not obvious over Dickinson in view of Smith.

Claim 14 as amended, recites:

A method of using an authentication server to authenticate a user to a third party server, the method comprising the third party server:

looking up a random record ID associated with the user, the random record ID used to separate the user's identity from authentication data;

generating a one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user;

receiving the authentication data, the authentication data being the decrypted one-time key decrypted with the user's private key by the authentication server, such that the user does not have control of the user's private key at any time; and

permitting access to the server.

As noted above, neither Dickinson nor Smith teach or suggest a record ID, nor the concept of separating the user's identity from the authentication data. Therefore, claim 14, and claims 15-16 which depend on it are not obvious over Dickinson in view of Smith.

Claim 17 as amended, recites:

A third-party authentication system comprising:

an authentication server to receive a record ID for a user, the record ID randomly generated to separate the user's identity from

authentication data and a one-time key generated by a third party server and encrypted with a user's public key by the third party server;

a comparison logic in the authentication server to receive the user authentication data from the client and determine whether the user's authentication data matches the record ID; and

a decryption logic in the authentication server to decrypt the one-time key with a private key associated with the validated record ID, and to return the decrypted one-time key to the client.

As noted above, neither Dickinson nor Smith teach or suggest a randomly generated record ID, nor the concept of separating the user's identity from the authentication data. Therefore, claim 17, and claims 18-31 which depend on it are not obvious over Dickinson in view of Smith.

Examiner rejected claims 7, 10, 25, and 28 under 35 U.S.C. §103(a) as being unpatentable over Dickinson as applied to claim 1 above, and further in view of U.S. Patent No. 6,581,161 to Byford.

Byford teaches the use of biometric data for authentication. However, Byford does not teach or suggest the use of a record ID in this context. Therefore, Byford does not overcome the shortcomings of Dickinson and Smith discussed above. Thus, claims 7, 10, 25, and 28 are not obvious over Dickinson in view of Byford.

Examiner rejected claims 15, 16, 18, and 21 under 35 U.S.C. §103(a) as being unpatentable over Dickinson as applied to claims 14 and 17 above, and further in view of U.S. Patent No. 5,692,106 to Towers et al.

Towers discusses the determination of authentication policy associated with a user. However, Towers does not teach or suggest the use of a record ID in this context. Therefore, Towers does not overcome the shortcomings of Dickinson and Smith discussed above. Thus, claims 7, 10, 25, and 28 are not obvious over Dickinson in view of Towers.

Examiner rejected claims 19 and 22 under 35 U.S.C. §103(a) as being unpatentable over Dickinson as applied to claim 17 above, and further in view of U.S. Patent No. 6,119,227 to Mao.

Mao discusses nonce generation to be included with user authentication data. However, Mao does not teach or suggest the use of a record ID in this context. Therefore, Towers does not overcome the shortcomings of Dickinson and Smith discussed above. Thus, claims 7, 10, 25, and 28 are not obvious over Dickinson in view of Mao.

Applicant respectfully submits that in view of the amendments and discussion set forth herein, the applicable rejections have been overcome. Accordingly, the present and amended claims should be found to be in condition for allowance.

If a telephone interview would expedite the prosecution of this application, the Examiner is invited to contact Judith Szepesi at (408) 720-8300.

If there are any additional charges/credits, please charge/credit our deposit account no. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 8/22/05

Judith A. Szepesi
Reg. No. 39,393

Customer No. 08791
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300